



JP20

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of

Takanori MASUI et al.

Group Art Unit: 2183

Application No.: 10/660,560

Filed: September 12, 2003

Docket No.: 117046

For: INFORMATION PROCESSOR AND INFORMATION PROCESSING METHOD FOR
COOPERATIVE OPERATION OF JOB PROCESSOR

CLAIM FOR PRIORITY

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested for the above-identified patent application and the priority provided in 35 U.S.C. §119 is hereby claimed:

Japanese Patent Application No. 2003-081918 filed March 25, 2003.

In support of this claim, a certified copy of said original foreign application:

☒ is filed herewith.

It is requested that the file of this application be marked to indicate that the requirements of 35 U.S.C. §119 have been fulfilled and that the Patent and Trademark Office kindly acknowledge receipt of this document.

Respectfully submitted,

James A. Oliff
Registration No. 27,075

Thomas J. Pardini
Registration No. 30,411

JAO:TJP/mps

Date: December 10, 2004

OLIFF & BERRIDGE, PLC
P.O. Box 19928
Alexandria, Virginia 22320
Telephone: (703) 836-6400

**DEPOSIT ACCOUNT USE
AUTHORIZATION**

Please grant any extension
necessary for entry;
Charge any fee due to our
Deposit Account No. 15-0461

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2003年 3月25日
Date of Application:

出願番号 特願2003-081918
Application Number:

[ST. 10/C]: [JP 2003-081918]

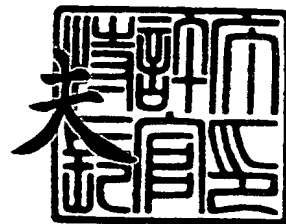
願人 富士ゼロックス株式会社
Applicant(s):

CERTIFIED COPY OF
PRIORITY DOCUMENT

2003年 9月10日

特許庁長官
Commissioner,
Japan Patent Office

今井 康



【書類名】 特許願

【整理番号】 FE03-00269

【提出日】 平成15年 3月25日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 12/00

【発明者】

 【住所又は居所】 神奈川県海老名市本郷 2 2 7 4 番地 富士ゼロックス株式会社海老名事業所内

 【氏名】 益井 隆徳

【発明者】

 【住所又は居所】 神奈川県海老名市本郷 2 2 7 4 番地 富士ゼロックス株式会社海老名事業所内

 【氏名】 佐竹 雅紀

【発明者】

 【住所又は居所】 神奈川県海老名市本郷 2 2 7 4 番地 富士ゼロックス株式会社海老名事業所内

 【氏名】 横濱 竜彦

【特許出願人】

 【識別番号】 000005496

 【氏名又は名称】 富士ゼロックス株式会社

【代理人】

 【識別番号】 100075258

 【弁理士】

 【氏名又は名称】 吉田 研二

 【電話番号】 0422-21-2340

【選任した代理人】

【識別番号】 100096976

【弁理士】

【氏名又は名称】 石田 純

【電話番号】 0422-21-2340

【手数料の表示】

【予納台帳番号】 001753

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報処理装置及び方法

【特許請求の範囲】

【請求項 1】 指示データに記述された処理記述に従って処理を実行する複数のジョブ処理装置を連携動作させることによりサービスを実現する情報処理装置であって、

前記指示データに記述された処理記述に対し、各ジョブ処理装置の実行対象となる部分に、実行するジョブ処理装置が復号可能に暗号化する暗号処理部と、

前記暗号処理部により処理記述が暗号化された指示データを、前記処理記述の表わす処理を実行するジョブ処理装置に伝達すべく送信する送信部とを備えることを特徴とする情報処理装置。

【請求項 2】 請求項 1 に記載の情報処理装置であって、

前記暗号処理部は、暗号化の対象とする処理記述より後に処理を実行すべき処理記述の暗号化データを含めて暗号化することを特徴とする情報処理装置。

【請求項 3】 請求項 1 に記載の情報処理装置であって、

前記暗号処理部は、暗号化の対象となる処理記述を実行するジョブ処理装置の公開鍵を用いて暗号化処理を施すことを特徴とする情報処理装置。

【請求項 4】 請求項 1 に記載の情報処理装置において、

前記暗号処理部は、各ジョブ処理装置の実行対象となる複数の部分について、それぞれ暗号化することを特徴とする情報処理装置。

【請求項 5】 請求項 4 に記載の情報処理装置において、

前記暗号処理部は、部分毎に異なる鍵で暗号化することを特徴とする情報処理装置。

【請求項 6】 複数のジョブ処理装置が所定の順序で連携動作することでサービスを実現するシステムにおいて、そのシステムを構成する情報処理装置であって、

処理の内容が記述された処理記述が暗号化された指示データを受信する受信部と、

前記受信部により受信された指示データに含まれる自装置の実行対象となる処

理記述の部分を復号化する復号処理部と、

前記復号処理部により復号化された処理記述を指示データから削除する削除部と、

前記削除部により処理記述が削除された指示データを、次に処理を実行するジョブ処理装置に向けて送信する送信部と
を備えることを特徴とする情報処理装置。

【請求項 7】 指示データに記述された複数の処理記述のそれぞれに従って処理を実行する複数のジョブ処理装置を連携動作させることによりサービスを実現するコンピュータが実行する情報処理方法であって、

前記指示データに記述された処理記述に対し、各ジョブ処理装置の実行対象となる部分に、実行するジョブ処理装置が復号可能に暗号化し、

暗号化された指示データを、前記処理記述の表わす処理を実行するジョブ処理装置に伝達すべく送信する
ことを特徴とする情報処理方法。

【請求項 8】 複数のジョブ処理装置が所定の順序で連携動作することでサービスを実現するシステムにおいて、そのシステムを構成するジョブ処理装置の少なくとも 1 つが実行する情報処理方法であって、

処理の内容が記述された処理記述が暗号化された指示データを受信し、

受信された指示データに含まれる自装置の実行対象となる処理記述の部分を復号化し、

復号化された処理記述を指示データから削除し、

処理記述が削除された指示データを、次に処理を実行するジョブ処理装置に向けて送信する
ことを特徴とする情報処理方法。

【請求項 9】 指示データに記述された複数の処理記述のそれぞれに従って処理を実行する複数のジョブ処理装置を連携動作させることによりサービスを実現するコンピュータのプログラムであって、

コンピュータに、

前記指示データに記述された処理記述に対し、各ジョブ処理装置の実行対象と

なる部分に、実行するジョブ処理装置が復号可能に暗号化する手順と、

暗号化された指示データを、前記処理記述の表わす処理を実行するジョブ処理装置に伝達すべく送信する手順と
を実行させるためのプログラム。

【請求項 10】 複数のジョブ処理装置が所定の順序で連携動作することでサービスを実現するシステムにおいて、そのシステムを構成するコンピュータのプログラムであって、

コンピュータに、

処理の内容が記述された処理記述が暗号化された指示データを受信する手順と

、
受信された指示データに含まれる自装置の実行対象となる処理記述の部分を復号化する手順と、

復号化された処理記述を指示データから削除する手順と、

処理記述が削除された指示データを、次に処理を実行するジョブ処理装置に向けて送信する手順と

を実行させるためのプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ネットワーク上に存在する様々な処理装置を連携させることで、多様な連携処理を実現するための技術に関し、特に連携処理におけるセキュリティ技術に関する。

【0002】

【従来の技術】

スキャナ、ファクシミリ装置、プリンタ、複写機、及びそれらの機能を統合した複合機を LAN（ローカルエリアネットワーク）に接続し、パーソナルコンピュータやメールサーバなどの情報処理装置と連携させ、オフィス作業用の各種サービスを提供するワークフローシステムが提案されている。

【0003】

また近年、インターネット上に散在する各種ウェブアプリケーションを連携させる技術が提案されている。インターネット上にある多様な提供者が提供するアプリケーションサービスを連結して1つのシステムを構成できると、様々な既存サービスを利用することができるのでシステム開発コストが大幅に低減できると期待されている。また、このような連携的なサービスを実現するための共通の基盤としてXML (eXtensible Markup Language)等の言語が注目されている。

【0004】

また、従来のワークフローシステムとしては、特許文献1や特許文献2、特許文献3に示されるものが知られている。

【0005】

【特許文献1】

特開平08-123744号公報

【特許文献2】

特開2002-099686号公報

【特許文献3】

特開2001-282970号公報

【0006】

【発明が解決しようとする課題】

連携サービスのためには、個々の処理装置に対し実行すべき処理を示した指示データを送る必要がある。インターネット上の処理装置を利用してワークフローを構成する場合、処理装置に対する指示データがインターネット上を流れることになる。しかしながら、従来のワークフローシステムは、このようなネットワークを流れる指示データのセキュリティに考慮を払っていない。

【0007】

また、連携サービスにおいて連携動作する複数の処理装置に対する指示データの提供の仕方として、例えばそれらすべての処理装置の指示データを1つの指示書にまとめて各処理装置に伝達する方式が考えられる。このような方式をとった場合、ある処理装置に対する指示データが他の処理装置にも伝わってしまう。すべての処理装置が同一社内のネットワーク上に存在する場合はこれでもさほど問

題はないが、インターネット上にある外部の処理装置に対して他の処理装置への指示データが漏洩することはセキュリティ上好ましくない。

【0008】

【課題を解決するための手段】

本発明は、指示データに記述された処理記述に従って処理を実行する複数のジョブ処理装置を連携動作させることによりサービスを実現する情報処理装置であって、前記指示データに記述された処理記述に対し、各ジョブ処理装置の実行対象となる部分に、実行するジョブ処理装置が復号可能に暗号化する暗号処理部と、前記暗号処理部により処理記述が暗号化された指示データを、前記処理記述の表わす処理を実行するジョブ処理装置に伝達すべく送信する送信部と、を備える情報処理装置を提供する。

【0009】

この情報処理装置は、後述する発明の実施の形態における指示入力装置として実現することもできるし、フロー制御装置として実現することもできる。

【0010】

また本発明の好適な態様では、前記暗号処理部は、暗号化の対象とする処理記述より後に処理を実行すべき処理記述の暗号化データを含めて暗号化する。

【0011】

また本発明は、複数のジョブ処理装置が所定の順序で連携動作することでサービスを実現するシステムにおいて、そのシステムを構成する情報処理装置であって、処理の内容が記述された処理記述が暗号化された指示データを受信する受信部と、前記受信部により受信された指示データに含まれる自装置の実行対象となる処理記述の部分を復号化する復号処理部と、前記復号処理部により復号化された処理記述を指示データから削除する削除部と、前記削除部により処理記述が削除された指示データを、次に処理を実行するジョブ処理装置に向けて送信する送信部とを備える。

【0012】

【発明の実施の形態】

以下、本発明の実施の形態（以下実施形態という）について、図面に基づいて

説明する。

【0013】

図1は、本発明に係るサービス提供システムのシステム構成パターンの一例を示す図である。このシステムは、指示入力装置10、フロー制御装置20、及び複数のアプリケーションサーバ25を含んでいる。

【0014】

アプリケーションサーバ25は、他の装置からの要求に応じて所定の処理サービスを提供するサーバである。例えば、サーバ25の例としては、例えば、文書データベースサーバや、メールサーバ、画像データに対して色変換や回転などの操作を施す画像処理サーバ等を挙げることができる。サーバ25は、そのような処理サービスを例えばウェブアプリケーションサービス等の形で提供する。

【0015】

このシステムは、あるサーバ25で文書を検索し、この結果検索された文書を別のサーバによって電子メールとして送信する、といった具合に、複数のサーバ25の処理を連携させた連携サービスを提供することができる。

【0016】

指示入力装置10は、このシステムに対するユーザの処理指示を入力するための装置である。ユーザは、指示入力装置10に対し、上述のような連携サービスの実行指示を入力することができる。指示入力装置10は、例えばパーソナルコンピュータに、ユーザから本システムへの指示の入力を受け付けるためのユーザインタフェースプログラムを組み込んだものでよい。しかしながら、オフィスにおける文書処理サービスを想定すると、情報処理機能や通信機能に加え、紙文書を読み取って電子データ化する機能をも備えるデジタル複合機を指示入力装置10として用いることが好適である。デジタル複合機は、スキャナ、プリンタ、複写機、ファクシミリ、ネットワーク通信等の機能を併せ持つ。

【0017】

フロー制御装置20は、各サーバ25に対して処理を依頼することで、それら個々のサーバ25が提供するサービスを連携した連携サービスを実現する。

【0018】

好適には、指示入力装置 10、フロー制御装置 20 及び各サーバ 25 は、公開鍵暗号方式に対応しており、各自の秘密鍵、公開鍵を有している。また、指示入力装置 10、フロー制御装置 20 及び各サーバ 25 は、他の装置 10、20 やサーバ 25 の公開鍵を保持しているか、又は必要に応じてネットワーク上の認証局から取得することができる。

【0019】

図 1 のシステムでは、ユーザが指示入力装置 10 に対して連携サービスの指示を入力すると、指示入力装置 10 がその指示内容を示したデータを送る。このデータ（以下ではフロー指示書 50 と呼ぶ）を、フロー制御装置 20 に送信する。このフロー指示書 50 には、連携サービスに関与するすべてのサーバの処理内容の記述と、それら各処理の実行順序の情報が含まれている。フロー指示書 50 を受信したフロー制御装置 20 は、その指示書 50 に従って各サーバ 25 を制御することで、その指示書 50 が示す連携サービスを実現する。

【0020】

このとき、フロー制御装置 20 は、受信したフロー指示書 50 に基づき各サーバ 25 への指示書（指示内容を示したデータ）52 を作成し、これら指示書 52 を各サーバ 25 に送ることで、それらサーバ 25 の連携動作を実現する。すなわち、フロー制御装置 20 は、フロー指示書 50 の記述に従い、次に動作させるべきサーバ 25 に対して指示書 52 を送信し、これに対してそのサーバ 25 から処理終了の通知（及び場合によっては処理結果のデータ）が返ってくると、その次のサーバ 25 に対して指示書 52 を送信する。

【0021】

このように図 1 のシステムは、サーバ 25 群がフロー制御装置 20 の制御の下に連携するという、いわばスター（星）型のシステム構成をとっている。

【0022】

次に、図 2 を参照して、本発明に係るサービス提供システムのシステム構成パターンの別の一例を説明する。図 2 において、図 1 に示したシステムの構成要素と同等の構成要素には同一符号を付して説明を簡略化する。

【0023】

このシステムは、指示入力装置 10 と複数のアプリケーションサーバ 25 とから構成されている。

【0024】

図 1 のシステムが連携制御のためのフロー制御装置 20 を有するのに対し、図 2 のシステムはそのような中央の制御装置を持たず、各アプリケーションサーバ 25 自身が連携動作のための制御動作を実行する。このため、指示入力装置 10 は、ユーザが指示した連携サービスのために各サーバ 25 が実行すべき処理を示したフロー指示書 50 を作成し、これを各サーバ 25 に送信して実行させる。

【0025】

図 2 の構成は、連携サービスを構成する各処理のための各サーバ 25 が、それぞれ各処理の順に並んだ、いわばデ이지チェーン（連鎖）型の構成となる。この構成では、サーバ連鎖の中の最初のサーバ 25-1 に対して指示入力装置 10 から指示書 50 を送信すると、これを契機にサービス処理が開始される。そして、サーバ 25-1 の処理が終了すると次のサーバ 25-2 の処理が開始され、このサーバ 25-2 の処理が終了するとその次のサーバ 25-3 の処理が開始されるといった具合に、各段階のサーバ 25 の間で処理が連携されていく。この場合、各サーバ 25 には、指示入力装置 10 から直接、又は前段のサーバ 25 から指示書 54 が送信される。そして、各サーバ 25 はその指示書に従って処理を実行するとともに、その指示書に示された次のサーバ 25 に対して処理開始の指示又は指示書 54 を送信する。このような仕組みで連携が実現される（詳細は後述）。

【0026】

以上、各サーバ 25 の連携の仕組みとして、フロー制御装置 20 により集中制御するフロー制御装置介在型と、各サーバ 25 が順に次のサーバ 25 に処理を受け渡すフロー制御装置非介在型の 2 つの仕組みを説明した。

【0027】

次に、連携サービスのために各サーバ 25 に送信される指示書 52, 54 についての 2 つのタイプを説明する。

【0028】

第 1 は、連携サービスに関与する各サーバ 25 に対し、当該サーバ 25 への指

示（該サーバ 25 の処理内容の記述）のみならず、他のサーバ 25 への指示をも含んだ指示書 52 又は 54 を送信する方式である。この方式の 1 つの例として、連携サービスに關与するすべてのサーバ 25 への指示を含んだ指示書を各サーバ 25 に送信する方式がある。このように、他のサーバ 25 への指示も含む形態の指示書を「包括指示書」と呼ぶこととする。

【0029】

第 2 は、連携サービスに關与する各サーバ 25 に対し、当該サーバ 25 への指示のみを含み、他のサーバ 25 への指示を含まない指示書 52 又は 54 を送信する方式である。このように、他のサーバ 25 への指示を含まないタイプの指示書を「個別指示書」と呼ぶこととする。

【0030】

これら指示書 52 又は 54 の 2 つのタイプと、前述のシステム構成の 2 つのタイプを組み合わせれば、各サーバ 25 への指示書の送信形態としていくつかの送信形態が得られる。そのうちの代表的なものとして次の 4 つの指示送信形態を挙げることができる。

【0031】

第 1 は、フロー制御装置介在型のシステムに包括指示書を適用したものであり、フロー制御装置 20 から各サーバ 25 に対して包括指示書 60 を送信する方式である。この形態の一例を図 3 に示す。

【0032】

図 3 の例では、サーバ 25-1 に対する指示内容を示した個別指示書 62-1 と、サーバ 25-2 に対する指示内容を示した個別指示書 62-2 と、サーバ 25-3 への指示内容を示した個別指示書 62-3 とを含んだ包括指示書 60 を、フロー制御装置 20 からそれら各サーバ 25-1, 25-2, 25-3 に送信する。この包括指示書 60 では、各個別指示書 62 が処理の実行順序に従って先頭から順に並べられている。この包括指示書 60 は、指示入力装置 10 からフロー制御装置 20 に送られるフロー指示書 50 の記述内容に基づき作成される。例えば、フロー指示書 50 は包括指示書 60 と同じ内容を記述したものでよい。

【0033】

この場合、フロー制御装置 2 0 は、まず連携サービスの最初のサーバ 2 5 - 1 に対して包括指示書 6 0 を送信する。サーバ 2 5 - 1 はその包括指示書 6 0 のうち自分宛の個別指示書 6 2 - 1 を解釈して処理を実行し、その処理結果をフロー制御装置 2 0 に返す。これを受けたフロー制御装置 2 0 は、次のサーバ 2 5 - 1 に対して包括指示書 6 0 を送信する。このような処理を繰り返すことで連携サービスを実現できる。

【 0 0 3 4 】

この変形として、フロー制御装置 2 0 から各サーバ 2 5 に送信する包括指示書 6 0 から、それまでに完了している処理についての記述を取り除く方式も好適である。この構成によれば、少なくとも処理が終わったサーバ 2 5 の処理内容は、後続のサーバ 2 5 に対して秘密にすることができる。

【 0 0 3 5 】

また、図 3 の指示送信形態の別の変形として、次のような方式も可能である。この方式では、まず連携サービスに関与するすべてのサーバ 2 5 への個別指示書 6 2 を含んだ包括指示書 6 0 をフロー制御装置 2 0 からそれら各サーバ 2 5 に送信する。そして、各サーバ 2 5 は、自分の前のサーバ 2 5 から処理開始指示が来るまでは処理を開始せず、その開始指示を受け取ると包括指示書 6 0 内の自分宛の個別指示書 6 2 に従って処理を実行し、自分の処理が終わるとその旨をフロー制御装置 2 0 に通知する。フロー制御装置 2 0 は、その通知を受けると、次のサーバに処理開始指示を出す。

【 0 0 3 6 】

第 2 の指示送信形態は、フロー制御装置介在型システムに個別指示書を適用したものであり、フロー制御装置 2 0 から各サーバ 2 5 に対し、それぞれ当該サーバ 2 5 に対応する個別指示書 6 2 を送信する。この一例を図 4 に示す。

【 0 0 3 7 】

図 4 の例では、フロー制御装置 2 0 は、指示入力装置 1 0 から受信したフロー指示書に基づき、サーバ 2 5 - 1 に対する指示内容を示した個別指示書 6 2 - 1 と、サーバ 2 5 - 2 に対する指示内容を示した個別指示書 6 2 - 2 と、サーバ 2 5 - 3 への指示内容を示した個別指示書 6 2 - 3 とをそれぞれ作成し、それら各

個別指示書 6 2 をそれぞれ対応するサーバ 2 5 に送信する。

【 0 0 3 8 】

第 3 の指示送信形態は、フロー制御装置非介在型システムに包括指示書を適用したものである。この形態の一例を図 5 に示す。

【 0 0 3 9 】

図 5 の形態では、図 3 の形態と同様の包括指示書 6 0 を、サーバ 2 5 - 1 からサーバ 2 5 - 2 へ、サーバ 2 5 - 2 からサーバ 2 5 - 3 へと受け渡す。すなわち、図 5 の例では、まず指示入力装置 1 0 からサーバ 2 5 - 1 に対し、包括指示書 6 0 と同内容のフロー指示書を送信する。サーバ 2 5 - 1 は、包括指示書 6 0 の中の自分宛の個別指示書 6 2 - 1 に示される処理を実行し、その処理が完了すると、同じ包括指示書 6 0（及び必要に応じてその処理の結果）を次のサーバ 2 5 - 2 に送信する。サーバ 2 5 - 2 は、包括指示書 6 0 を受け取ると、自分宛の個別指示書 6 2 - 2 に示される処理を実行し、その処理が完了すると、同じ包括指示書 6 0（及び必要に応じてその処理の結果）を次のサーバ 2 5 - 3 に送信する。このようにして、各サーバ 2 5 による処理の連携が実現される。

【 0 0 4 0 】

図 5 の指示送信形態の変形として、各サーバ 2 5 が処理を終えると、自分が実行した処理についての記述（すなわち自分宛の個別指示書 6 2）を包括指示書 6 0 から取り除き、残りの個別指示書 6 2 からなる包括指示書を作成して次のサーバ 2 5 に送信する構成も好適である。この構成によれば、少なくとも処理が終わったサーバ 2 5 の処理内容は、後続のサーバ 2 5 に対して秘密にすることができる。

【 0 0 4 1 】

また、図 5 の送信指示形態の別の変形として、次のような方式も可能である。この方式では、まず連携サービスに関与するすべてのサーバ 2 5 への個別指示書 6 2 を含んだ包括指示書 6 0 を指示入力装置 1 0 からそれら各サーバ 2 5 に送信する。そして、各サーバ 2 5 は、自分の前のサーバ 2 5 から処理開始指示が来るまでは処理を開始せず、その開始指示を受け取ると包括指示書 6 0 内の自分宛の個別指示書 6 2 に従って処理を実行し、自分の処理が終わると次のサーバに処理

開始指示を出す。包括指示書 6 0 では、各サーバ 2 5 の個別指示書 6 2 が処理の順に並んでいるので、各サーバ 2 5 は前後の個別指示書 6 2 の記述から自分の前段のサーバ 2 5 や後段のサーバ 2 5 を識別することができ、上記のような処理の流れを実現できる。

【 0 0 4 2 】

第 4 の指示送信形態は、フロー制御装置非介在型システムに個別指示書を適用した方式である。この方式の一例を図 6 に示す。

【 0 0 4 3 】

図 6 の例では、指示入力装置 1 0 から、連携サービスに関与する各サーバ 2 5 - 1, 2 5 - 2, 2 5 - 3 に対し、それぞれ当該サーバ 2 5 に対応する個別指示書 6 2 - 1, 6 2 - 2, 6 2 - 3 を送信する。そして、各サーバ 2 5 宛の個別指示書 6 2 には、当該サーバ 2 5 の前後の各サーバ 2 5 (又は指示入力装置 1 0) を示す情報が含まれている。そして、各サーバ 2 5 は、前段のサーバ 2 5 から処理開始指示を受けて初めてその個別指示書 6 2 の処理を開始し、処理が終了すると後段のサーバ 2 5 に対して処理開始指示を送る。このような仕組みにより、サーバ 2 5 間の連携を実現できる。

【 0 0 4 4 】

以上に説明した指示送信形態のうち、各サーバ 2 5 に個別指示書 6 2 を送信する第 2 及び第 4 の形態では、インターネット等のネットワーク上で個別指示書 6 2 の内容を盗聴されるリスクがある。

【 0 0 4 5 】

また、各サーバ 2 5 に包括指示書 6 0 を送る第 1 及び第 3 の形態では、ネットワーク上での盗聴のリスクに加え、各サーバ 2 5 への指示内容が他のサーバ 2 5 に漏洩するリスクがある。例えば、ある企業が連携サービスのために、自社のサーバ 2 5 以外に他社が提供するインターネット 5 0 上のサーバ 2 5 を用いる場合、自社サーバ 2 5 への指示内容が他社サーバ 2 5 に知られたくないことが少なくない。

【 0 0 4 6 】

以下、このような各サーバ 2 5 に送る指示書についてのセキュリティ上のリス

クを軽減するための仕組みについて説明する。

【 0 0 4 7 】

この仕組みの基本的な考え方は、サーバ 2 5 に対する個別指示書 6 2 に対し、連携サービスに関与するサーバ 2 5 群の中でそのサーバ 2 5 のみが復号可能な暗号化処理を施すというものである。

【 0 0 4 8 】

各サーバ 2 5 に対して対応する個別指示書 6 2 のみを送信する上記第 2 及び第 4 の指示送信形態では、このような暗号化により、ネットワーク上での指示内容の漏洩リスクを軽減できる。

【 0 0 4 9 】

また、各サーバ 2 5 に対して包括指示書 6 0 を送信する上記第 1 及び第 3 の指示送信形態では、包括指示書 6 0 に含まれるべき各個別指示書 6 2 に対し、それぞれ対応するサーバ 2 5 にのみ復号可能な暗号化処理を施し、それら暗号化された個別指示書を処理実行順序に従って並べた包括指示書 6 0 を作成する。これにより、各サーバ 2 5 に対する個別指示書 6 2 の内容がネットワーク上で盗聴されるリスクを軽減できると共に、他のサーバ 2 5 に漏洩するリスクも軽減できる。

【 0 0 5 0 】

いずれの場合も、個別指示書 6 2 の暗号化処理としては、共通鍵暗号方式を利用した暗号化処理を用いることもできるし、公開鍵暗号方式を利用した暗号化処理を用いることもできる。共通鍵暗号方式を用いる場合は、各サーバ宛の個別指示書 6 2 を作成するフロー制御装置 2 0 又は指示入力装置 1 0 と、当該指示書 6 2 の送り先のサーバ 2 5 とが、暗号・復号化のための共通鍵を有していればよい。一方、公開鍵暗号方式を用いる場合は、各サーバ 2 5 宛の個別指示書 6 2 を作成するフロー制御装置 2 0 又は指示入力装置 1 0 が、それら各サーバ 2 5 の公開鍵を有しているか、それら公開鍵をネットワーク上の鍵管理サーバや認証局から取得する機能を有していればよい。また、個別指示書 6 2 を暗号化するセッション鍵（共通鍵）を乱数から生成して、そのセッション鍵で個別指示書 6 2 を暗号化すると共に、その暗号化されたセッション鍵を各サーバ 2 5 の公開鍵で暗号化して、暗号化された個別指示書 6 2 と一緒に送付してもよい。

【0 0 5 1】

なお、フロー制御装置 2 0 を用いる上記第 1 及び第 2 の指示送信形態では、処理の開始に当たり、指示入力装置 1 0 からフロー制御装置 2 0 に対してフロー指示書 5 0 を送る必要がある。この場合、指示入力装置 1 0 が、フロー制御装置 2 0 のみが復号可能な暗号化処理（例えばフロー制御装置 2 0 の公開鍵を用いた暗号化）を用いてそのフロー指示書 5 0 を暗号化し、この結果得られる暗号化された指示書をフロー制御装置 2 0 に送信する。フロー制御装置 2 0 は、受け取った指示書を復号し、この復号化結果に基づき各サーバ 2 5 宛の個別指示書 6 2 （第 2 又は第 4 の形態）又は包括指示書 6 0 （第 1 又は第 3 の形態）を作成する。

【0 0 5 2】

次に、連携サービスの具体例を用いて、本実施形態における指示書の暗号化処理について説明する。

【0 0 5 3】

ここでは、具体例として、図 7 に示すように、ページばらし（文書ファイルをページ単位のファイルに分割し、要求されたページのファイルを返す処理）のサービスを提供するサーバ 2 5 a と、電子メール送信サービスを提供するサーバ 2 5 b を含むシステムを想定する。サーバ 2 5 a は“pagedivider.foo.jp”というホスト名を有し、サーバ 2 5 b は“mailsender.foo.jp”というホスト名を有するとする。そして、このシステムで、指示入力装置 1 0 で読み取った複数のページを有する紙原稿のうちの第 1 ページのデータを、所定の宛先に電子メールで送信するというサービス（以下、便宜上「サービス A」と呼ぶ）を実現するとする。サービス A では、指示入力装置 1 0 にて紙原稿の読み取りが行われ、サーバ 2 5 a にて読み取り結果の文書ファイルから第 1 ページが抽出され、サーバ 2 5 b にてその第 1 ページのファイルを含んだ電子メールが作成され、所定宛先に送られることになる。また、この例では、指示送信形態として、図 5 に例示した第 3 の形態を用いるものとする。

【0 0 5 4】

この場合、指示入力装置 1 0 は、そのサービス A の内容を示す包括指示書 6 0 0 を作成する。図 8 に、この包括指示書 6 0 0 の例を示す。

【 0 0 5 5 】

この例の包括指示書 6 0 0 は、XML (eXtended Markup Language) で記述されている。この包括指示書 6 0 0 は、この指示書 6 0 0 で使用している XML のバージョンや文字コードを示す文書要素 6 0 5 と、この指示書 6 0 0 が表す連携サービスを示す文書要素 6 1 0 とを含んでいる。連携サービスを示す要素 6 1 0 のタグには、この連携サービスの名称 (name="report delivery") が示されている。そして、この要素 6 1 0 には、それら連携サービスを担う各サーバ 2 5 a, 2 5 b に対する個別指示書 6 2 0 a, 6 2 0 b とが記述されている。

【 0 0 5 6 】

個別指示書 6 2 0 a の記述 6 2 2 a には、連携サービス中での当該処理の順番 (order="1")、及び当該処理を実行するサーバ 2 5 a のホスト名 (url="pagedivider.foo.jp") が示されている。また、記述 6 2 4 a の 1 行目には、そのサーバ 2 5 a が提供する各種の処理のうち、今回利用する処理の名称 (jobname="ExtractFrontPage") が示される。例えば、サーバ 2 5 a は、文書ファイルから先頭ページを取り出してその先頭ページのファイルを作成する処理の他に、文書ファイルをページ単位にばらして各ページごとのファイルを作成する処理などの様々な処理ができる。記述 6 2 4 a の 1 行目は、それら様々な処理のうち、文書ファイルの先頭ページのファイルを作成する処理を示すものである。また記述 6 2 4 a の 2 行目及び 3 行目にはその処理のパラメータが示されている。2 行目のパラメータは、その処理に対する入力ファイルのファイル名 ("ExtractFrontPage") を示し、3 行目のパラメータはその処理の出力ファイルのファイル名 ("ExtractedPage") である。指示入力装置 1 0 が、読み取った原稿を示す文書ファイルに対し、"ExtractFrontPage" というファイル名を付し、この指示書 6 0 0 に添付して送信すれば、サーバ 2 5 a でそのファイルが処理対象であると認識できる。

【 0 0 5 7 】

また、個別指示書 6 2 0 a は、この指示書が示す処理の後に処理を行うサーバ 2 5 b を示す記述 6 2 6 a を含んでいる。この記述 6 2 6 a には、次のサーバ 2 5 b のホスト名 (url="pagedivider.foo.jp") が示されている。

【 0 0 5 8 】

サーバ 2 5 b に対する個別指示書 6 2 0 b は、上記個別指示書 6 2 0 a と同様、処理の順序及びサーバ 2 5 b のホスト名を示す記述 6 2 2 b と、そのサーバ 2 5 b が行うべき処理の名称及びその処理のパラメータを示す記述 6 2 4 b を含んでいる。サーバ 2 5 b が行う処理は、電子メールの送信処理なので、パラメータとしては電子メールの宛先アドレス（記述 6 2 4 b の 2 行目）と、その電子メールに添付されるファイルの名称（記述 6 2 4 b の 3 行目）とを含んでいる。なお、添付されるファイルの名称は、サーバ 2 5 a の処理の出力ファイル名と同じものとなっている。

【 0 0 5 9 】

なお、サーバ 2 5 b は、この包括指示書 6 0 0 が示す連携サービスの中の最後の処理なので、次のサーバを示す記述は含まれていない。

【 0 0 6 0 】

図 8 に示した包括指示書 6 0 0 では、各個別指示書 6 2 0 a, 6 2 0 b 内の処理内容を示す記述 6 2 4 a, 6 2 4 b が平文で記述されているので、このままネットワーク上に送信すると、盗聴のリスクがあるとともに、2 番目のサーバ 2 5 b の処理内容が最初のサーバ 2 5 a に知られてしまうことになる。例えば、処理内容の記述の中に、ユーザのクレジットカード番号などがパラメータとして含まれる場合などには、その情報が関係するサーバ以外に漏れることは望ましくない。また、その処理内容全体を関係するサーバ以外に秘匿したい場合もある。

【 0 0 6 1 】

そこで、図 7 の例では、指示入力装置 1 0 が、その包括指示書 6 0 0 の各個別指示書 6 2 0 a, 6 2 0 b のうちの処理内容を示す記述 6 2 4 a, 6 2 4 b を、それぞれ対応するサーバ 2 5 a, 2 5 b の公開鍵を用いて暗号化する。このような暗号化処理を経た包括指示書の例を図 9 に示す。図 9 において、図 8 と同内容の記述には、図 8 と同じ符号を付して説明を省略する。

【 0 0 6 2 】

図 9 に示す包括指示書 7 0 0 は、W 3 C の規格である “XML E n c r y p t i o n” に従ったものである。この包括指示書 7 0 0 において、サーバ 2 5 a に対する個別指示書 7 2 0 a は、処理の順序及びサーバ 2 5 b のホスト名を示す

記述 6 2 2 a と、次に処理を行うサーバ 2 5 b を示す記述 6 2 6 a と、暗号化部分 7 2 4 a とを含んでいる。この暗号化部分 7 2 4 a は、平文の個別指示書 6 2 0 a の処理内容の記述 6 2 4 a を、サーバ 2 5 a の公開鍵を用いて暗号化したデータを含む。記述 7 2 5 a のタグ "<CipherValue>" と "</CipherValue>" とに挟まれた ASCII コードの文字列が、その暗号化データの値を示している。暗号化部分 7 2 4 a の最初のタグには、その暗号化データを生成するのに使用した暗号化方式を示す情報 ("Type='http://www.w3.org/2001/04/xmlenc#Element' xmlns='http://www.w3.org/2001/04/xmlenc#'") が記述されている。なお、説明を簡単にするために図 9 では省略しているが、この暗号化データを生成するのに用いた公開鍵を示す鍵情報の要素 ("<KeyInfo>") がその暗号化部分 7 2 4 a 内に記述されている。

【 0 0 6 3 】

同様に、サーバ 2 5 b に対する個別指示書 7 2 0 b には、処理の順序及びサーバ 2 5 b のホスト名を示す記述 6 2 2 b と、処理内容 6 2 4 b をサーバ 2 5 b の公開鍵で暗号化したデータの記述 7 2 5 b を含んだ暗号化部分 7 2 4 b とを有する。

【 0 0 6 4 】

図 9 に示した包括指示書 7 0 0 を用いれば、ネットワーク上で仮にその包括指示書 7 0 0 が盗聴されても、各サーバ 2 5 a 、 2 5 b の処理内容はその暗号が解読されない限り知られない。また、サーバ 2 5 a やサーバ 2 6 b がこの包括指示書 7 0 0 を受け取った場合、自分宛の個別指示書の暗号化部分 7 2 4 a 、 7 2 4 b は自分の秘密鍵で復号できるが、他のサーバに対する個別指示書の暗号化部分は復号できない。

【 0 0 6 5 】

図 7 のシステムでは、指示入力装置 1 0 が、上述の包括指示書 7 0 0 を作成し、付属のスキャナで読み取った原稿の文書ファイルをその指示書 7 0 0 と共にサーバ 2 5 a に送信する。これらのデータを受け取ったサーバ 2 5 a は、指示書 7 0 0 中の処理順序及びホスト名の記述 6 2 2 a 及び 6 2 2 b の平文記述を調べることで、自分宛の個別指示書 6 2 0 a を識別する。次にその個別指示書 6 2 0 a

の中の暗号化部分 7 2 4 a を自分の秘密鍵で復号する。この復号結果は、図 8 に示した処理内容の記述 6 2 4 a となる。そして、暗号化部分 7 2 4 a を復号結果の記述 6 2 4 a に置き換えることで、平文の個別指示書 6 2 0 a を復元し、この指示書 6 2 0 a を先頭から順に解釈していき、その解釈に応じた処理を実行する。この例では、サーバ 2 5 a は、入力された文書ファイルから先頭ページを取り出す処理を実行し、その先頭ページのファイルに所定のファイル名 "ExtractedPage" をつける。このようにして、要求されたサービス処理を完了すると、サーバ 2 5 a は、作成した先頭ページのファイルと包括指示書 7 0 0 とを、記述 6 2 6 a に従って次のサーバ 2 5 b に送信する。

【 0 0 6 6 】

サーバ 2 5 b は、サーバ 2 5 a と同様に、受け取った包括指示書 7 0 0 から自分宛の個別指示書 7 2 0 b を識別し、その中の暗号化部分 7 2 4 b を自分の秘密鍵で復号することで平文の個別指示書 6 2 0 b を復元し、その平文指示書 6 2 0 b に示された処理を実行する。この場合サーバ 2 5 b は、先頭ページのファイル "ExtractedPage" を添付した電子メールを作成し、平文指示書 6 2 0 b に記述された宛先 ("person1@foo.co.jp") に対して送信する。

【 0 0 6 7 】

以上では、説明を分かりやすくするために非常に単純な例を挙げたが、もっと複雑な処理にも本実施形態の仕組みは適用可能である。例えば、この例の拡張として、例えばユーザが読み取った文書の先頭ページをユーザの属するグループのリーダーに、全ページをそのグループの同僚複数人に送信するといった定型処理も同様に実現可能である。この場合は、サーバ 2 5 a に対する個別指示書 6 2 0 a には、文書ファイルから第 1 ページを抽出すると共に、第 1 ページのファイルとその文書ファイルとをサーバ 2 5 b に送るという処理内容が記述され、サーバ 2 5 b に対する個別指示書 6 2 0 b には、受け取った第 1 ページのファイルをグループリーダーの所定のメールアドレスに送信し、全ページのファイルを各同僚の所定のメールアドレスに送信するという処理内容が記述される。暗号化については、上記の例と同様でよい。

【 0 0 6 8 】

このような仕組みによれば、各個別指示書 6 2 0 a, 6 2 0 b の処理内容が第三者に盗聴されたり、その処理を実行するサーバ以外のサーバに漏れたりする可能性を大幅に低減できる。

【 0 0 6 9 】

なお、以上のシステムにおいて、指示入力装置 1 0 がサーバ 2 5 a の処理の対象である文書データをそのサーバ 2 5 a の公開鍵で暗号化してから送信したり、サーバ 2 5 a がサーバ 2 5 b の処理の対象である先頭ページのデータをそのサーバ 2 5 b の公開鍵で暗号化したりすれば、それら処理対象のデータをネットワーク上の第三者から保護することが可能である。

【 0 0 7 0 】

以上に説明した図 9 の例では、各個別指示書の処理内容の記述 6 2 4 a を暗号化したが、次のサーバの示す記述 6 2 6 a を併せて暗号化しても問題ない。個別指示書は、その個別指示書がどのサーバ宛のものなのかが特定できる情報のみ平文で記述しておけば、他の情報についてはすべて暗号化しても構わない。

【 0 0 7 1 】

また、サーバ 2 5 a は、次のサーバ 2 5 b に包括指示書 7 0 0 を送る代わりに、その包括指示書 7 0 0 から自分宛の個別指示書 7 2 0 b を除いた指示書を作成し、これをサーバ 2 5 b に送る構成としても良い。

【 0 0 7 2 】

図 7 ～図 9 に示した例は、指示送信形態として、図 5 に例示した第 3 の形態を用いた場合の例であったが、図 3 に示した第 1 の形態を用いる場合もこれと同様、図 9 に示すような暗号化された包括指示書 7 0 0 を各サーバ 2 5 に送るようにすればよい。ただし、このケースでは、各個別指示書の暗号化はフロー制御装置 2 0 にて行うこともできる。この場合、指示入力装置 1 0 は、フロー制御装置 2 0 に対し、包括指示書 6 0 0 の連携サービスを示す文書要素 6 1 0 全体をそのフロー制御装置 2 0 の公開鍵で暗号化したものを送信することで、包括指示書 6 0 0 全体の秘密を保持することができる。フロー制御装置 2 0 はそれを自分の秘密鍵で復号したあと、個々の個別指示書 6 2 0 a、6 2 0 b を対応するサーバ 2 5 a, 2 5 b の公開鍵で暗号化し、包括指示書 7 0 0 を作成する。この包括指示書

700を用いた各サーバ25の制御は、上述の通りでよい。

【0073】

また図4に示した第2の指示書送信形態を用いる場合は、各サーバ25には個別指示書のみを送ればよいので、フロー制御装置20にて、その個別指示書の中の処理内容等の記述を宛先のサーバ25の公開鍵で暗号化すればよい。この暗号化により生成される個別指示書の記述は、例えば、図9に示した包括指示書700を、個別指示書720aを1つしか含まないようにしたものでよい。

【0074】

図6に示した第4の指示書送信形態を用いる場合も各サーバ25には個別指示書のみを送ればよいので、指示入力装置10にて、第2の形態と同様、その個別指示書の中の処理内容等の記述を宛先のサーバ25の公開鍵で暗号化すればよい。

【0075】

以上、本実施形態における、各指示送信形態に対応する指示書データの秘密保護の方式について説明した。

【0076】

次に、包括指示書60の変形例について説明する。この変形例の包括指示書は、特に第3の指示送信形態において有益なものである。

【0077】

図10は、この変形例における包括指示書80のデータ構造を説明するための図である。この指示書80が適用されるシステム構成は、図5を参照されたい。

【0078】

この包括指示書80は、連携サービスの各処理を担う各サーバ25-1, 25-2, 25-3に対する各個別指示書62-1, 62-2, 62-3を、それら各処理の順序に従った入れ子構造となるように暗号化する。

【0079】

より詳しくは、まず連携サービスのフローの最後のサーバ25-3宛の個別指示書62-3を該サーバ25-3の公開鍵で暗号化し、暗号化データ82-3を作成する。この暗号化では、個別指示書62-3のうち、この指示書の処理を実

行するサーバを示す記述（例えば図 8 の記述 6 2 2 a）を除く部分を暗号化する。もちろん、暗号化する箇所をその部分よりも更に絞り込んでもよい。

【0080】

次に、最後のサーバ 2 5 - 3 の 1 つ前のサーバ 2 5 - 2 宛の個別指示書 6 2 - 2 と、その暗号化データ 8 2 - 3 とを併せたものを、サーバ 2 5 - 2 の公開鍵で暗号化することで、暗号化データ 8 2 - 2 を作成する。

【0081】

そして、その 1 つ前のサーバ 2 5 - 1 宛の個別指示書 6 2 - 1 とその暗号化データ 8 2 - 2 とを併せたものを、サーバ 2 5 - 1 の公開鍵で暗号化することで、暗号化データ 8 2 - 1 を作成する。

【0082】

このような処理を、連携サービスのフローにおける先頭のサーバの個別指示書を暗号化するまで再帰的に繰り返す。すなわち、この暗号化処理では、暗号化の対象とする処理記述（すなわち個別指示書）に、その記述より後に処理を実行すべき処理記述の暗号化データを含めて暗号化する。そして、この暗号化処理を、実行順序が最後の処理記述から順に再帰的に適用する。

【0083】

図 10 の例では、サーバ 2 5 - 1 が先頭のサーバなので、この暗号化の最終結果は暗号化データ 8 2 - 1 となる。この最終の暗号化データ 8 2 - 1 に対し、連携サービスの指示書である旨を示す記述（図 8 の記述 6 0 5 や文書要素 6 1 0 の開始タグ及び終了タグ）を付加することで、包括指示書 8 0 が完成する。

【0084】

この入れ子構造の包括指示書の具体例を図 11 に示す。この例は、図 8 に示す平文の包括指示書 6 0 0 に対応するものである。この指示書が適用されるシステム構成としては、図 7 の構成を参照されたい。

【0085】

図 11 に示す包括指示書 8 0 0 は、XML のバージョン等の記述 6 0 5 と連携サービスの名称の記述 6 1 5 の後に、入れ子構造で暗号化された暗号化データ 8 2 0 を含む文書要素 8 1 0 を含んでいる。この文書要素 8 1 0 の先頭には、連携

サービスの先頭のサーバ 2 5 a のホスト名を含んだタグ 8 1 5 が示されている。暗号化データ 8 2 0 は、使用した暗号方式を示す記述と、入れ子構造の暗号化の最終的な暗号化結果の値の記述 8 2 5 を含んでいる。

【 0 0 8 6 】

指示入力装置 1 0 は、このような包括指示書 8 0 0 を作成し、連携サービスの先頭のサーバ 2 5 a に送信する。これを受信したサーバ 2 5 a は、平文で記述された”<wrapinstruction>”タグ 8 1 5 内のホスト名から、その指示書 8 0 0 が自分宛であることを認識し、その中の記述 8 2 5 に示される暗号化結果の値を自分の秘密鍵を用いて復号する。これにより、復号結果 8 3 0 が得られる。

【 0 0 8 7 】

復号結果 8 3 0 は、そのサーバ 2 5 a 宛の平文の個別指示書 6 2 0 a と、後続のサーバ 2 5 群宛の入れ子構造の暗号化データ 8 5 0 を含んだ文書要素 8 4 0 が含まれる。

【 0 0 8 8 】

サーバ 2 5 a は、その平文の個別指示書 6 2 0 a に従って処理を実行する。そして、処理が完了すると、記述 6 2 6 a に示される次のサーバ 2 5 b に対する指示書を作成し、その指示書とその処理の結果とをサーバ 2 5 b に送信する。このとき、次のサーバ 2 5 b への指示書は、復号結果 8 3 0 から処理済みの自分宛の個別指示書 6 2 0 a を削除することで作成できる。すなわち、その指示書には、指示書であることを示す記述 6 0 5 及び 6 1 5 と、暗号化データ 8 5 0 を含む文書要素 8 4 0 が含まれることになる。

【 0 0 8 9 】

この指示書を受け取ったサーバ 2 5 b は、その文書要素 8 4 0 中に含まれるホスト名の記述 6 2 2 b からその指示書が自分宛であることを認識し、記述 8 5 5 に含まれる暗号化結果の値を自分の秘密鍵で復号する。これにより、図 7 の指示書における、処理内容の記述 6 2 4 b（図 8 参照）に対応する平文記述を得ることができる。サーバ 2 5 b は、その記述 6 2 4 b に従って処理を実行する。

【 0 0 9 0 】

なお、図 1 1 の例では、サーバ 2 5 b が連携サービスの最後のサーバであった

ため、文書要素 840 は”<service>”タグで示される文書要素として表された。このかわりに、サーバ 25 a の次のサーバ 25 b が連携サービスの最後でなければ、文書要素 840 は、最初の包括指示書 800 の文書 810 と同様、”<wrapinstruction>”タグによって示されることとなる。なお、連携サービスの最後のサーバ宛の個別指示書も、他のサーバ宛の各段階の暗号化結果と同様、指示書全体を暗号化し、その暗号化結果”<wrapinstruction>”タグで囲むようにしてももちろんよい。

【0091】

このように、指示入力装置 10 で入れ子構造の包括指示書 800 を作成する構成とすれば、あるサーバ宛の個別指示書は連携サービスのフローの中でそのサーバより前のすべてのサーバにより順に復号処理を受けない限り復号できない。したがって、連携サービスの先頭のサーバ以外のあるサーバ X が、自分の前段のサーバ以外から予め包括指示書を取得したとしても、そのサーバ X は復号ができないので処理を開始することができない。

【0092】

このような仕組みを利用すれば、あるサーバ X が、連携サービスのフローに従った処理を経ずに、勝手に処理を始めてしまうことを防止することができる。例えば、サーバ X が課金を伴う処理を行う場合、正しい処理フローを経ずに、前もって処理を始めて課金を開始すると、連携サービスを要求したユーザにとって好ましくないが、この入れ子構造の包括指示書 800 を用いることで、そのような状況が起こるのを抑止できる。

【0093】

以上、本実施形態のシステムの構成及び動作について説明した。以上の実施形態では、連携サービスのための個々の処理についての指示を、その処理を実行するサーバ 25 のみが復号可能な暗号処理で暗号化した。このときの暗号処理の単位となる「サーバ」は、あるサービス処理を記述したアプリケーションプログラムをコンピュータで実行させることにより実現される仮想機械であってもよいし、そのようなアプリケーションプログラムを 1 乃至複数備えたハードウェア装置であってもよい。すなわち、前者の場合アプリケーションごとに異なる暗号処理

を用い、後者の場合はハードウェア装置ごとに異なる暗号処理を用いることになる。アプリケーションごとの異なる暗号処理の例としては、アプリケーションごとにそれぞれ個別に秘密鍵・公開鍵ペアを割り当てて、公開鍵暗号方式を用いる仕組みを挙げることができる。ハードウェア装置ごとに異なる暗号化処理も同様である。ハードウェア装置単位の暗号処理を採用する場合、ハードウェア装置に対する個別指示書としては、連携サービス中でハードウェア装置内の各アプリケーションが連続して実行する処理の内容を順に記述したものとなる。指示入力装置 10 又はフロー制御装置 20 は、その個別指示書をそのハードウェア装置に対応する暗号処理にて暗号化する。

【0094】

次にこのシステムを構成する指示入力装置 10、フロー制御装置 20 及び各サーバ 25 の内部構成の一例を、図 12 を参照して説明する。

【0095】

まず、指示入力装置 10 について説明する。指示入力装置 10 の UI（ユーザ・インタフェース）102 は、指示入力装置 10 の状態や操作メニュー等を表示し、これに対するユーザの選択やパラメータ入力を受け取るユーザ・インタフェース機構であり、例えば液晶タッチパネルやテンキーボタン、各種の指示ボタンを備える。処理モジュール 104 は、当該指示入力装置 10 自体がユーザに提供するサービス処理を実行する処理モジュールである。指示入力装置 10 が複合機である場合、処理モジュール 104 には、スキャン機能、プリント機能、コピー機能、ファクシミリ送受信機能等を実現する機能モジュールが含まれる。この場合、これら処理モジュール 104 は、スキャンエンジンやプリントエンジン、ファクシミリ装置等のハードウェアと、それら各ハードウェアを制御するソフトウェアの組合せにより構成される。通信制御部 106 は、この指示入力装置 10 と LAN 等のネットワーク 35 上の他の装置との通信のための各種制御処理を行う機能モジュールである。

【0096】

暗号・復号処理部 108 は、指示入力装置 10 からネットワーク 35 に送信するデータに対して暗号化を行ったり、送信されてきた暗号化されたデータを復号

したりする機能モジュールである。ここでは、暗号・復号処理部 108 は、暗号方式として公開鍵暗号方式をサポートしているものとする。ただし、これは一例であり、暗号・復号処理部 108 は、共通鍵方式など他の暗号方式を基礎とするものであってもよい。

【0097】

暗号・復号処理部 108 で用いる暗号化処理の一例としては、乱数等で発生したセッション鍵（共通鍵）を用いて対象となる文書データを暗号化し、このセッション鍵を送信先の公開鍵で暗号化し、これら両暗号化データを送信先へに送信するという処理を挙げることができる。受信側では、受け取ったデータを自らの秘密鍵で復号することでセッション鍵を得、暗号化された文書データをそのセッション鍵により復号する。本明細書中で「公開鍵で暗号化する」といった場合、文字通り公開鍵を用いて対象データを暗号化する場合のみならず、このようなセッション鍵を利用する暗号化処理の場合もあるものとする。

【0098】

また、暗号・復号処理部 108 は、送信するデータに対して電子署名を施したり、受信したデータに付された電子署名を検証したりする機能を備える。電子署名は、例えば署名対象の文書データから MD5 (RFC1321) や SHA-1 (RFC3174) 等の所定ダイジェスト方式に従って求めたメッセージダイジェストを、署名者の秘密鍵で暗号化することにより得られる。この電子署名の検証は、該署名データを署名者の公開鍵で復号し、その復号化結果が、署名対象の文書データから所定ダイジェスト方式に従って求めたメッセージダイジェストと一致するか否かを判定することにより行われる。一致すれば、該文書データが署名者からの真正なデータであることが証明されると共に、該文書データに対して改竄が加えられていないことが証明される。

【0099】

ここで暗号・復号処理部 108 は、少なくともフロー制御装置 20 の公開鍵を保管している。また暗号・復号処理部 108 に、各サーバやユーザの公開鍵をネットワーク上の所定の認証局等から必要に応じて取得する機能を設けることも好適である。また暗号・復号処理部 108 は、該指示入力装置 10 自身の秘密鍵を

備え、該指示入力装置 10 の電子署名を行うことができる。

【0100】

上述の第3及び第4の指示送信形態（図5及び図6）の場合、各サーバ25に送信する指示書に対する上述の暗号化処理は、この暗号・復号処理部108にて実行される。また、第1及び第2の指示送信形態（図3及び図4）の場合でも、フロー制御装置20に対して送るフロー指示書50に対する暗号化処理は、この暗号・復号処理部108により実行される。

【0101】

トークン I/F（インタフェース）110は、ユーザが保持するハードウェアトークンを受け入れ、このトークンと通信することで該ユーザの秘密鍵による電子署名を取得する機構である。ここでハードウェアトークンは、ユーザが携帯する小型の認証デバイスである。公開鍵暗号方式を利用する場合、ハードウェアトークンは、例えば、ユーザの秘密鍵データを記憶する記憶チップと、署名対象のデータに対してユーザの秘密鍵を用いて暗号化を施すことにより署名データを生成する演算回路と、署名対象のデータの入力及び署名データの出力のためのインタフェース機構とを備えるものとなる。ハードウェアトークンは、例えば接触読み取り式又は非接触読み取り式の IC カード、USB (Universal Serial Bus) 等の各種有線インタフェース規格に対応したデバイス、或いはBluetooth等の各種無線インタフェース規格に対応したデバイスなどとして構成される。

【0102】

この構成では、通信制御部106は、送信すべきデータに対してユーザの電子署名を行う必要がある場合、例えばMD5などの方式に従ってそのデータのメッセージダイジェストを作成し、これをトークン I/F 110に装着されたハードウェアトークンに入力する。ハードウェアトークンは、入力されたメッセージダイジェストを、保持しているユーザの秘密鍵で暗号化し、その暗号化処理結果（すなわちユーザの署名）を通信制御部106に返す。このユーザ署名を通信制御部106が文書データに付加することにより、文書データに対するユーザの電子署名が為される。

【0103】

以上ではユーザのハードウェアトークンを利用してユーザの電子署名を行う方法を説明したが、別の方式として、指示入力装置 10 内にユーザの秘密鍵を予め保管しておき、この秘密鍵を用いて上述と同様の処理により該ユーザの電子署名を行う方式も可能である。この方式では、ユーザの秘密鍵保護のため、ユーザにパスワードやバイオメトリクス等の認証情報の入力を求め、これによりユーザ認証が成功した場合に限り、そのユーザの電子署名を認めるという制御を必須とする。ハードウェアトークンを用いる構成の場合、ユーザ署名が必要な連携サービスを行うと、最悪の場合その連携サービスが完了するまで指示入力装置 10 にトークンをセットしたまま待っている必要があるが、指示入力装置 10 に秘密鍵を保管する構成ではそのような待機は必要ない。逆に、ハードウェアトークンを用いる構成は、ユーザは、どの複合機その他の装置からでも、ユーザ署名が必要な連携サービスを実行できるという利点がある。

【0104】

以上、指示入力装置 10 の構成の一例を説明した。このような指示入力装置 10 は、コンピュータや上述の複合機など、プログラムを実行して情報処理を実行することができる装置に、上述の各種の機能を記述したプログラムを実行させることによって実現できる。

【0105】

次に、フロー制御装置 20 の構成について説明する。これは、上述の第 1 及び第 2 の指示送信形態（図 3 及び図 4 参照）に対応するものであり、第 3 及び第 4 の送信指示形態（図 5 及び図 6 参照）の場合は、このフロー制御装置 20 は必要ない。

【0106】

フロー制御装置 20 において、ユーザ管理部 202 は、該装置 20 がサービス対象とするユーザについての各種情報を管理している。ユーザ管理部 202 が管理する情報には、例えばユーザの認証に用いる認証情報（パスワードやバイオメトリクス情報など）や、ユーザが登録している UI 画面情報などがある。すなわち、本実施形態のシステムでは、ネットワーク 35 上の各種サーバ装置が提供するサービスをユーザが組み合わせることで、ユーザ固有の連携サービスを定義可

能としており、これらユーザ固有の連携サービスを指示できる該ユーザ固有の U I 画面をフロー制御装置 2 0 から提供する。

【0 1 0 7】

この場合、ユーザ（個人の場合もあれば、複数人からなるグループの場合もある）が指示入力装置 1 0 に認証情報を入力して認証が成功すると、指示入力装置 1 0 がフロー制御装置 2 0 に当該ユーザの U I 画面を要求する。この要求に応じ、フロー制御装置 2 0 は、そのユーザが登録した連携サービスのメニュー等を含んだ U I 画面を、そのユーザの公開鍵で暗号化した上で指示入力装置 1 0 に送信する。ユーザが、指示入力装置 1 0 のディスプレイに表示されたその U I 画面上で、使用したい連携サービスを選択すると、その選択内容がフロー制御装置 2 0 の公開鍵で暗号化された上で、指示入力装置 1 0 からフロー制御装置 2 0 に送られる。この選択結果を受けとったフロー制御装置 2 0 は、ユーザが選択した連携サービスを示す包括指示書のひな形データを、ユーザの公開鍵で暗号化した上で、指示入力装置 1 0 に送信する。指示入力装置 1 0 は、この包括指示書のひな形の中に、ユーザが入力しなければならないパラメータが含まれる場合、そのパラメータの入力画面を U I 1 0 2 に表示し、ユーザの入力を求める。このようにしてパラメータ群が入力されると、包括指示書が完成する。これが上述のフロー指示書 5 0 に対応する。指示入力装置 1 0 は、完成したフロー指示書をフロー制御装置 2 0 の公開鍵で暗号化した上で、フロー制御装置 2 0 に送信する。

【0 1 0 8】

ユーザによるフロー制御装置 2 0 への連携サービスの登録処理や、フロー制御装置 2 0 から指示入力装置 1 0 に提供する各ユーザ固有の U I 画面の情報については、本実施形態の要旨とは直接関係しないので説明を省略するが、これらについては本出願人による特願 2 0 0 2 - 2 7 5 2 2 9 号、特願 2 0 0 2 - 2 7 5 2 3 0 号、特願 2 0 0 2 - 2 7 5 2 3 1 号に開示されているので、必要があれば参照されたい。

【0 1 0 9】

なお、この例は、U I 画面の情報や連携サービスの包括指示書のひな形はフロー制御装置 2 0 が保管し、随時指示入力装置 1 0 に提供する構成であったが、そ

れら U I 画面や包括指示書のひな形を指示入力装置 1 0 に保管しておくこともできる。

【0 1 1 0】

フロー制御部 2 0 4 は、ユーザが要求した連携サービスを実現するために、連携サービスにおいて規定されるフローに従って各サーバ 2 5 や指示入力装置 1 0 に対して必要な処理の実行依頼を行う機能モジュールである。すなわち、連携サービスは、各サーバ 2 5 が提供する 1 以上の処理（以下では単位ジョブとも呼ぶ）からなるフローとして定義され、フロー制御装置 2 0 は、このフロー定義に示される単位ジョブを順に対応するサーバに依頼していく。ここで、各サーバの処理結果は、必要に応じてフロー制御装置 2 0 に返され、次の単位ジョブの処理対象データとしてフロー制御装置 2 0 から対応するサーバへと送信される。フロー制御部 2 0 4 は、このような各サーバ、複合機への処理依頼と、これに対する処理結果の取得などの処理を実行する。

【0 1 1 1】

なお、指示入力装置 1 0 が、連携サービスの指示受付機能の他にも処理機能を備え、この処理機能を連携サービスのために提供できる場合もある。この場合、指示入力装置 1 0 は、その処理機能についてはアプリケーションサーバ 2 5 の 1 つととらえることができる。

【0 1 1 2】

暗号・復号処理部 2 0 6 は、フロー制御装置 2 0 からネットワーク 3 5 に送信する文書データに対して暗号化を行ったり、送信されてきた暗号化データを復号したりする機能モジュールであり、暗号・復号処理部 1 0 8 と同等の暗号化、復号化、電子署名及びその検証の機能を有する。

【0 1 1 3】

ここで暗号・復号処理部 2 0 6 は、指示入力装置 1 0 や各サーバ 2 5 などの装置や、各ユーザの公開鍵を保管しているか、又はネットワーク上の認証局等から取得する機能を備える。そして、データを送信する必要が生じた場合は、その送信先の装置やユーザの公開鍵を用いて暗号化を行う。

【0 1 1 4】

上述の第 1 及び第 2 の指示送信形態（図 3 及び図 4）の場合、各サーバ 2 5 に送信する指示書に対する上述の暗号化処理は、この暗号・復号処理部 2 0 6 にて実行される。

【0 1 1 5】

また、電子署名機能については、暗号・復号処理部 2 0 6 は、フロー制御装置 2 0 の秘密鍵を備え、送信するデータに対してフロー制御装置 2 0 の電子署名を付することができる。

【0 1 1 6】

通信制御部 2 1 2 は、フロー制御装置 2 0 とネットワーク 3 5 上の他の装置との通信のための各種制御処理を行う機能モジュールである。

【0 1 1 7】

以上、フロー制御装置 2 0 の構成の一例を説明した。このようなフロー制御装置 2 0 は、上述の各種の機能を記述したプログラムをコンピュータに実行させることによって実現できる。

【0 1 1 8】

次にアプリケーションサーバ 2 5 について説明する。アプリケーションサーバ 2 5 は、該サーバが提供するサービスのためのアプリケーションプログラム 2 5 2 と、ネットワーク 3 5 上の他の装置との通信のための制御処理を実行する通信制御部 2 5 4 と、その通信の際の暗号化及び復号の処理を実行する暗号・復号処理部 2 5 6 とを備える。

【0 1 1 9】

サーバ 2 5 の暗号・復号処理部 2 5 6 は、指示入力装置 1 0，フロー制御装置 2 0 又は他のサーバ 2 5 から送られてきた指示書を上述のごとく復号する機能を備える。アプリケーション 2 5 2 はその復号の結果を受け取り、これを解釈し、その解釈の結果に応じた処理を実行する。

【0 1 2 0】

また暗号・復号処理部 2 5 6 は、該サーバ 2 5 の処理によって得られたデータを暗号化する機能を備える。そのような処理結果のデータを、フロー制御装置 2 0 又は他のサーバ 2 5 に送る際には、その送り先の公開鍵を用いてそのデータを

暗号化する。

【0 1 2 1】

また、通信制御部 2 5 4 は、上述の第 1 及び第 2 の指示送信形態（図 3 及び図 4）では、アプリケーション 2 5 2 の処理結果をフロー制御装置 2 0 に送信する処理を行う。また通信制御部 2 5 4 は、第 3 の指示送信形態（図 5）では、次のサーバ 2 5 に対する包括指示書 6 0（及び、必要に応じ、処理結果のデータ）を送信するための上述の処理を実行し、第 4 の指示送信形態（図 6）では、次のサーバ 2 5 に対する処理開始指示を送信するための上述の処理を実行する。

【0 1 2 2】

以上説明した指示入力装置 1 0 及びサーバ 2 5、及びフロー制御装置介在型のシステム構成の場合は更にフロー制御装置 2 0 により、上述の連携サービスのフローが実現されると共に、そのフローにおける各サーバ 2 5 への指示書の秘密を守る処理が行われる。

【図面の簡単な説明】

【図 1】 連携サービスを提供するシステムの構成の一例を示す図である。

【図 2】 連携サービスを提供するシステムの構成の別の例を示す図である。

。

【図 3】 連携サービスにおける各サーバへの指示書の送信形態の一例を示す図である。

【図 4】 連携サービスにおける各サーバへの指示書の送信形態の別の例を示す図である。

【図 5】 連携サービスにおける各サーバへの指示書の送信形態の更に別の例を示す図である。

【図 6】 連携サービスにおける各サーバへの指示書の送信形態の更に別の例を示す図である。

【図 7】 紙原稿を読み取って得た文書ファイルから先頭ページのみを取り出し、これを電子メールに添付して所定の宛先に送信するという連携サービスを実現するシステムの構成例を示す図である。

【図 8】 図 7 のシステムにおいて、指示入力装置がまず用意する平文の包

括指示書の例を示す図である。

【図 9】 図 9 の平文の包括指示書内の個々の指示を、その指示を実行するサーバの公開鍵で暗号化した結果を示す図である。

【図 1 0】 入れ子構造で暗号化した包括指示書の構造を示す模式図である。

【図 1 1】 入れ子構造で暗号化した包括指示書の一例を示す図である。

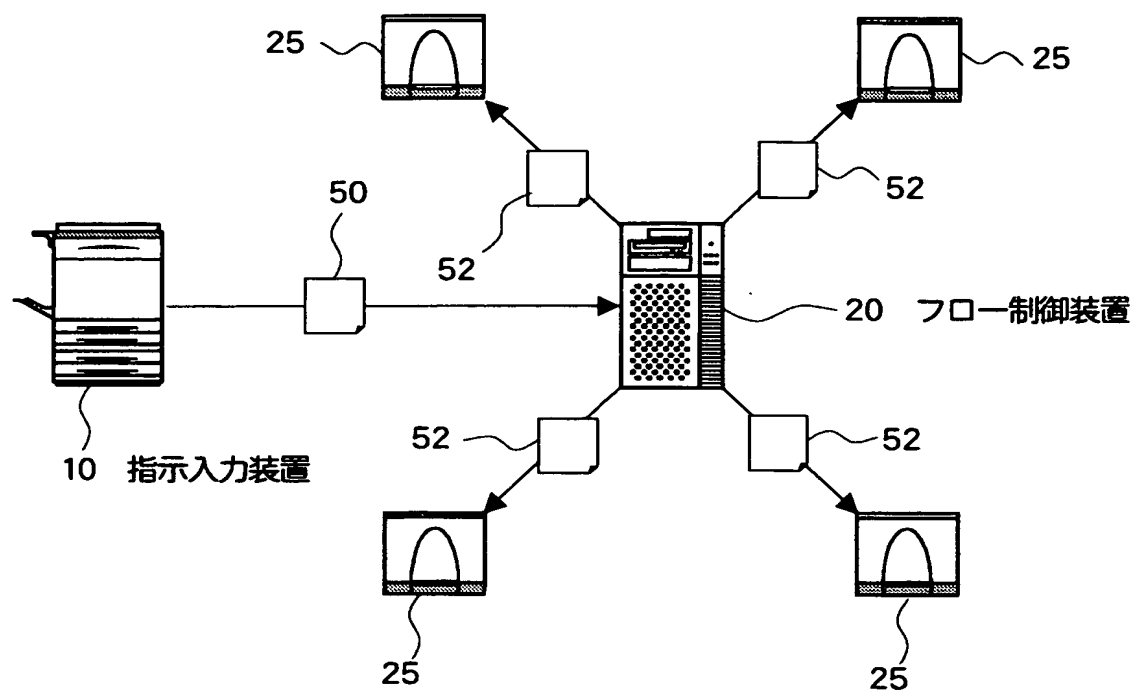
【図 1 2】 連携サービスを提供するシステムを構成する各装置の内部構造の例を示す図である。

【符号の説明】

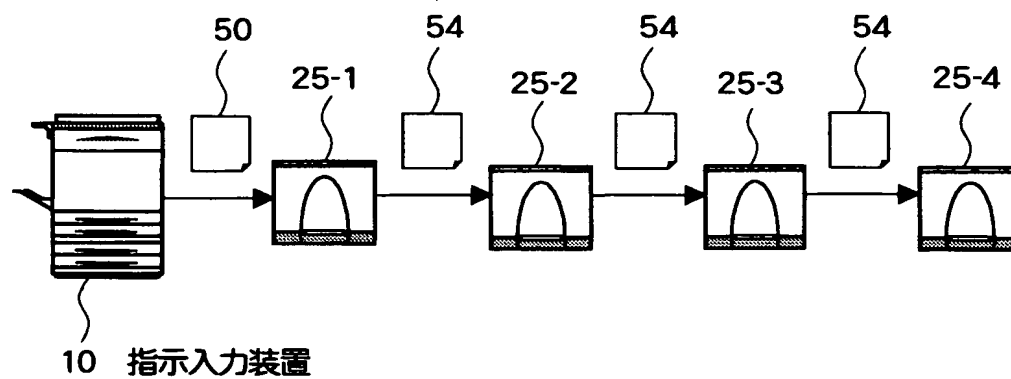
1 0 指示入力装置、2 0 フロー制御装置、2 5 アプリケーションサーバ、5 2, 5 4 指示書、6 0 包括指示書、6 2 個別指示書。

【書類名】 図面

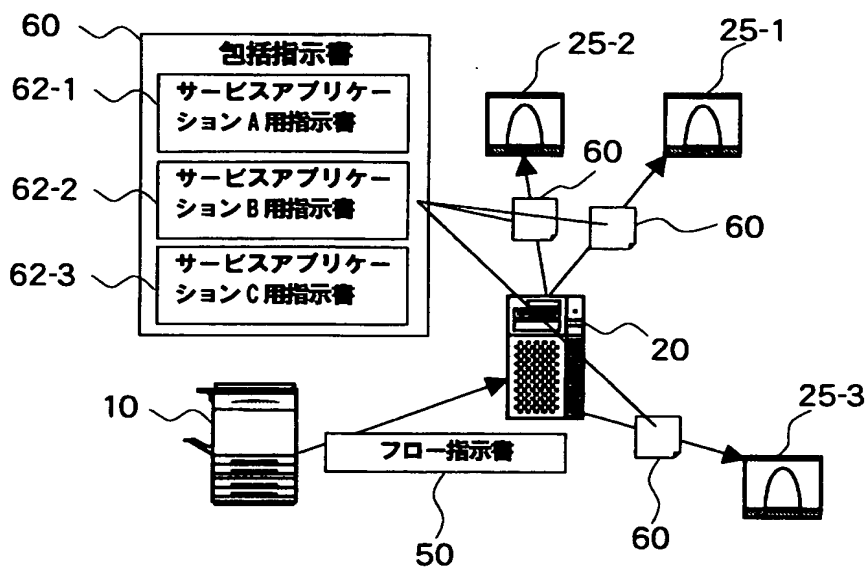
【図 1】



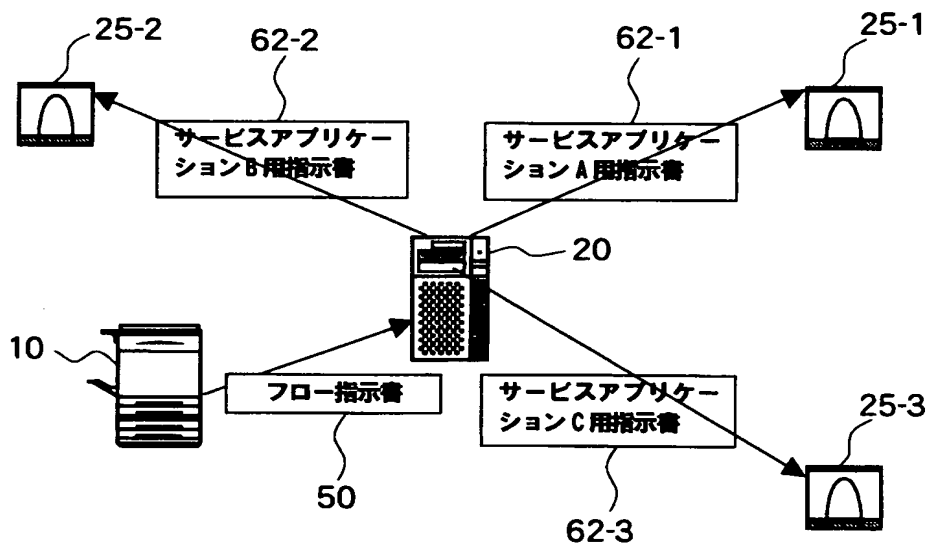
【図 2】



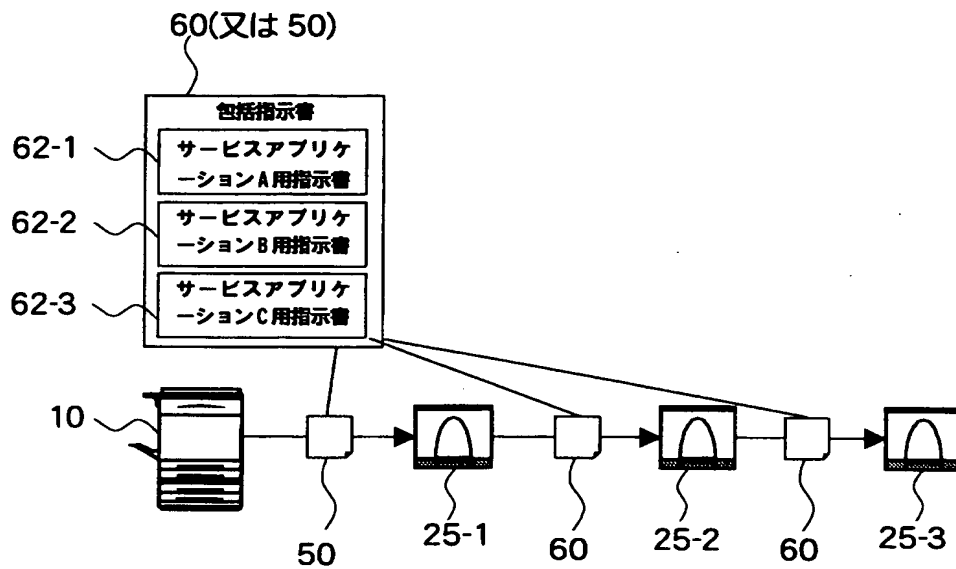
【図 3】



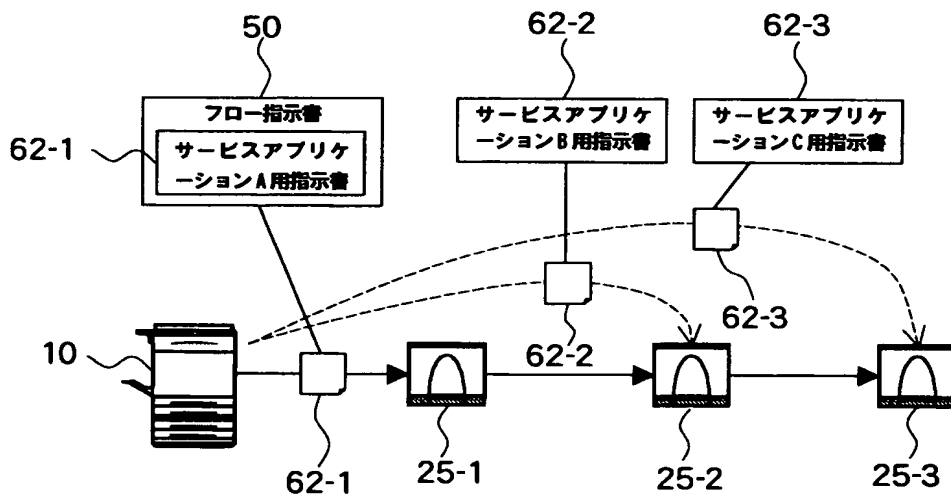
【図 4】



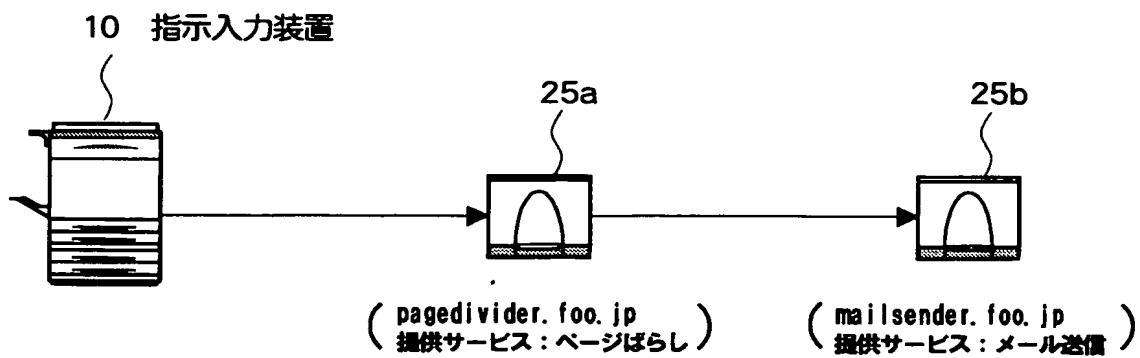
【図 5】



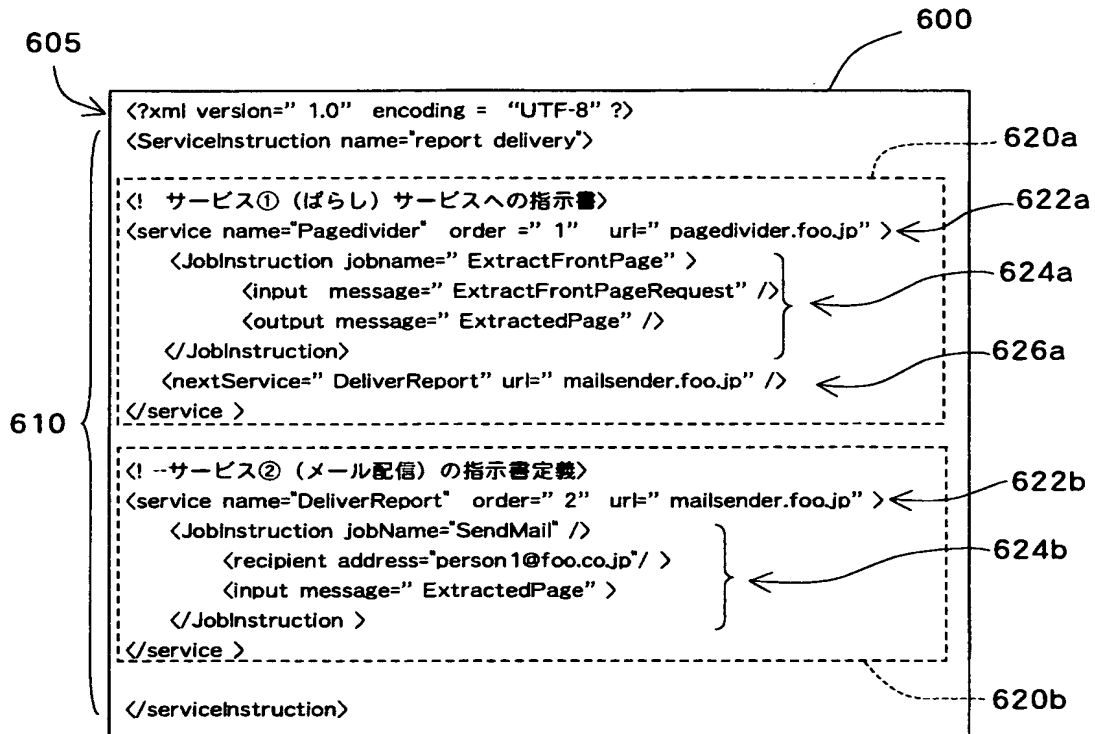
【図 6】



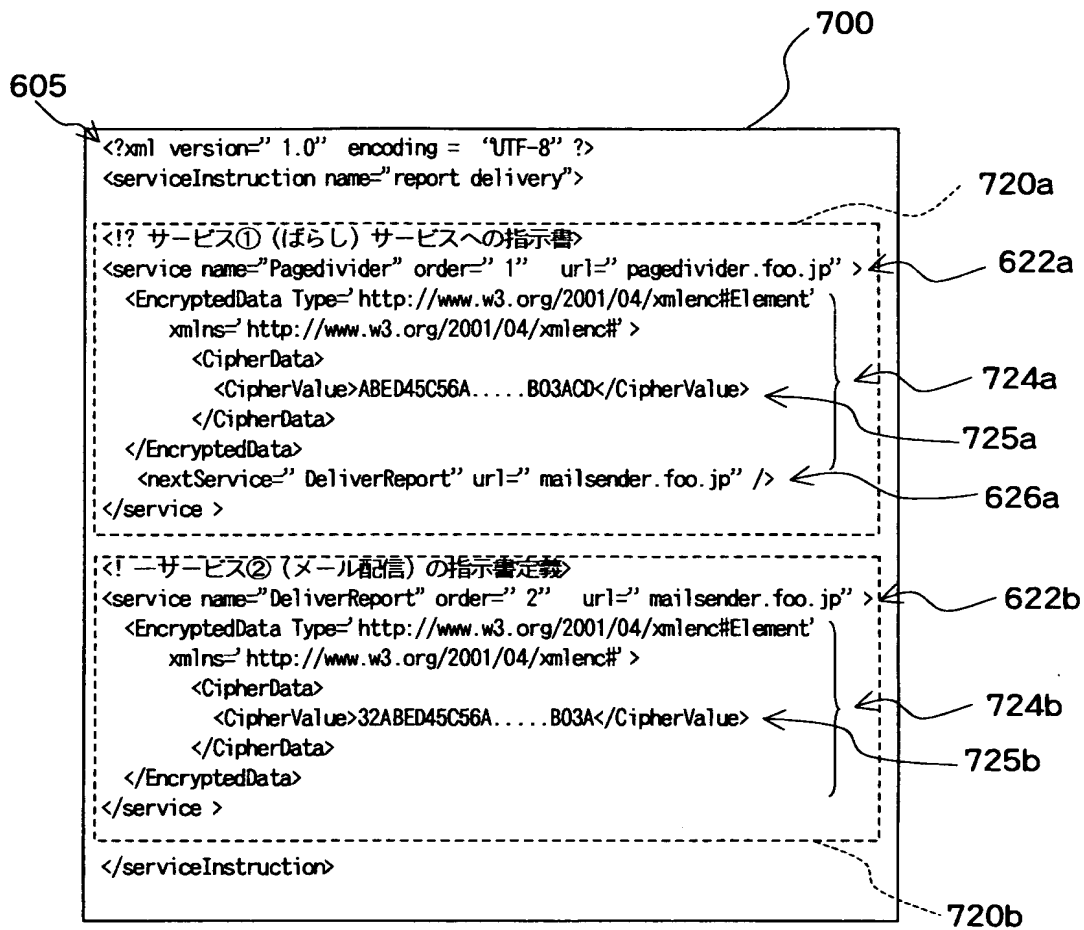
【図 7】



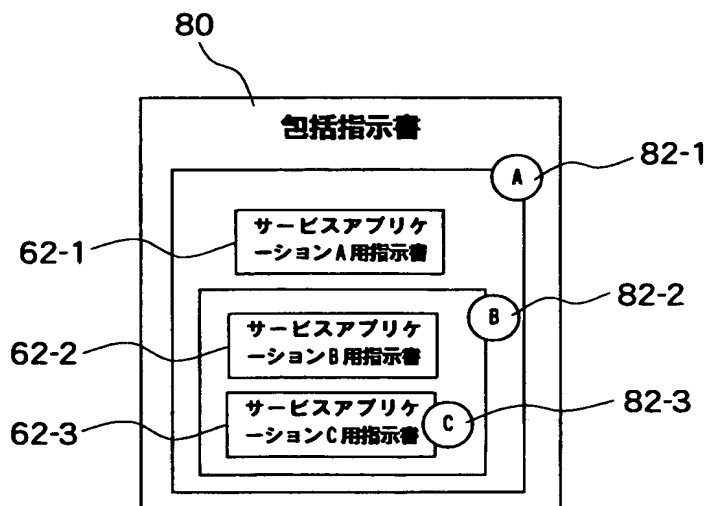
【図 8】



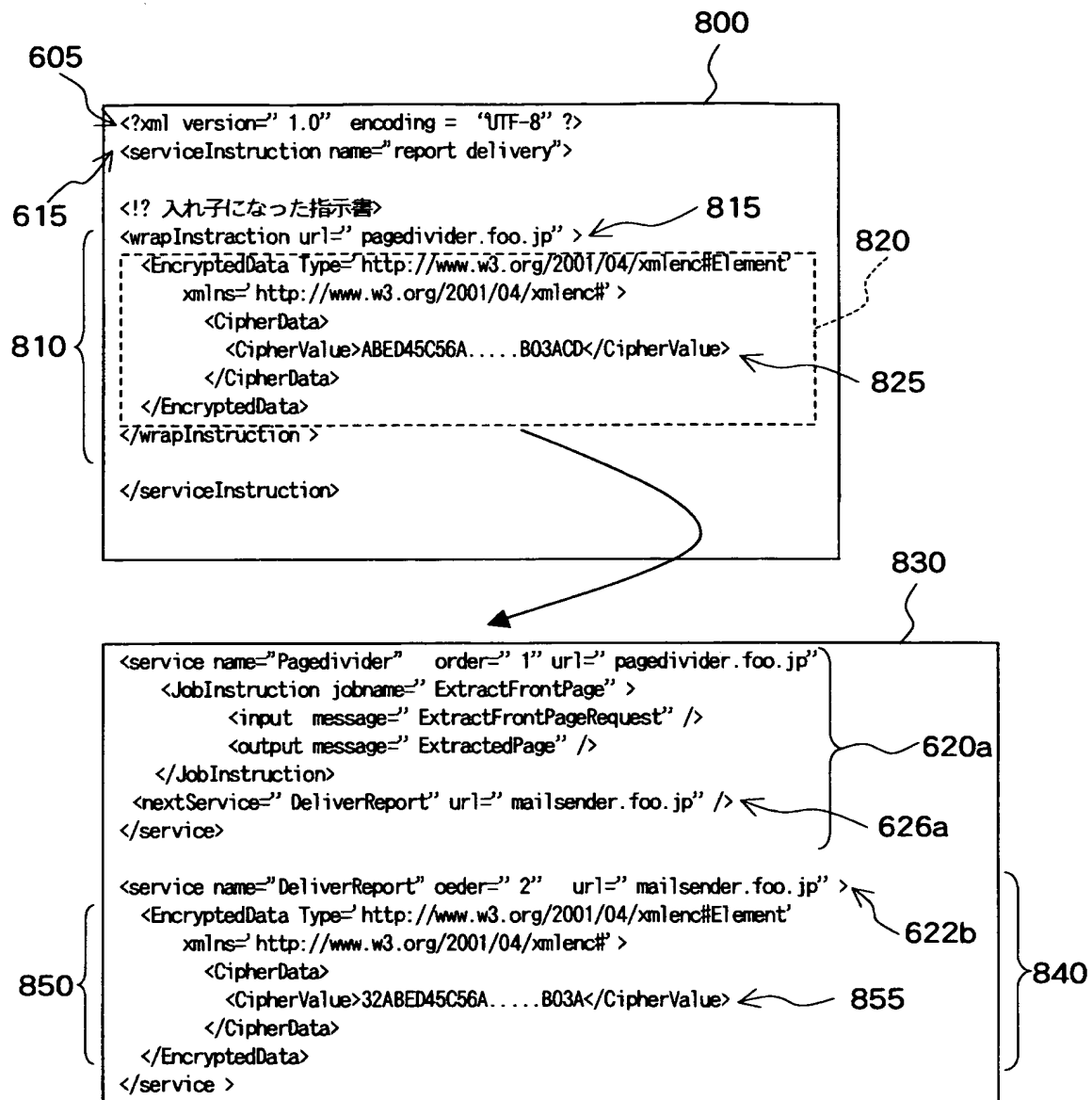
【図 9】



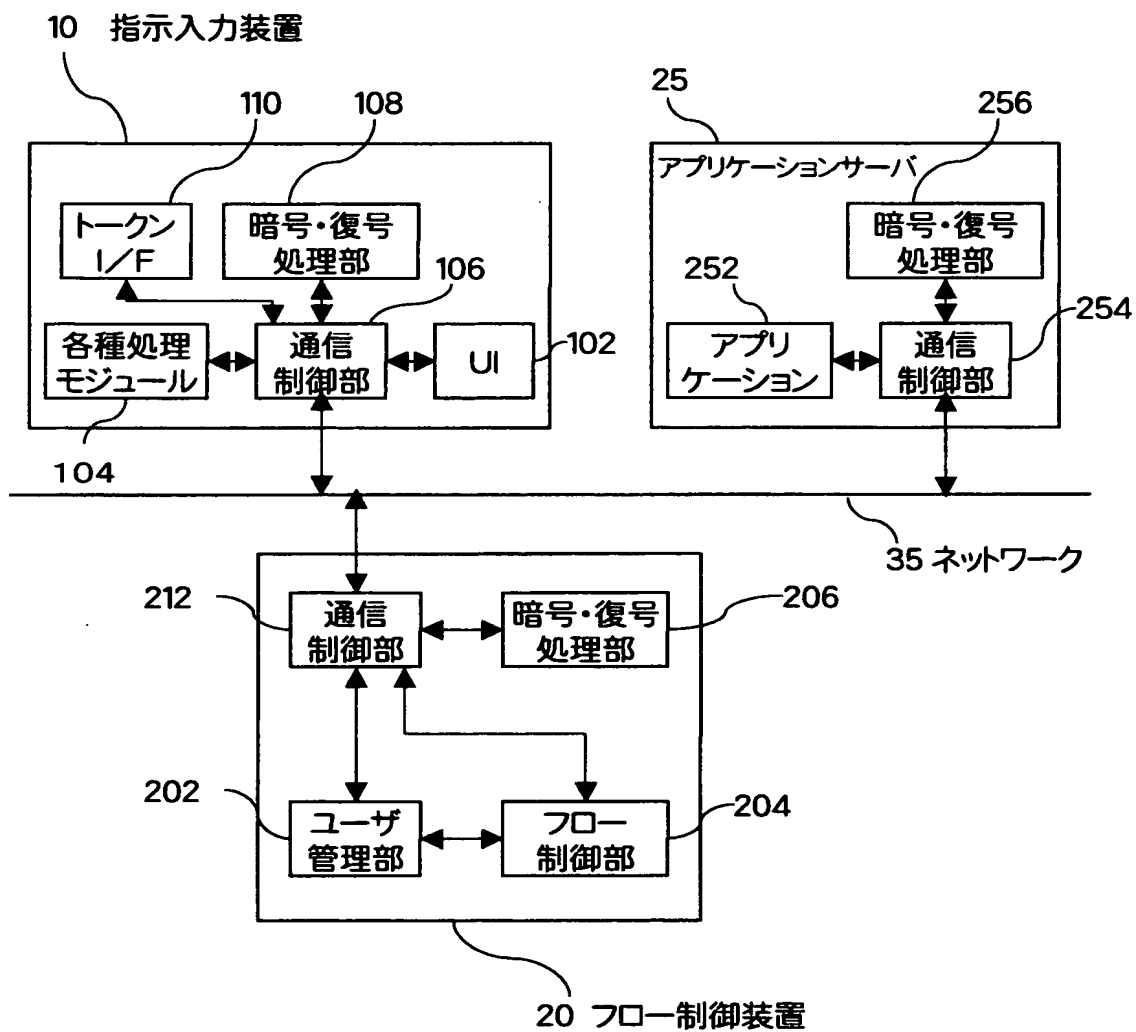
【図 10】



【図 11】



【図 12】



【書類名】 要約書

【要約】

【課題】 各サーバへの指示を示した指示書をそれらサーバ間で受け渡ししながら、各サーバが指示書内の各自の指示を実行することで、1つのサービスを提供するシステムにおいて、指示書に示された各サーバへの指示の秘密を守る。

【解決手段】 サーバ 2 5 a が提供するページばらし（複数ページを含む文書のファイルから所定のページを抜き出し、そのページのファイルを出力する処理）と、サーバ 2 5 b が提供する電子メール送信処理とを組み合わせることで、ユーザが指示入力装置 1 0 に投入した文書のファイルから、先頭ページを抜き出して、所定の宛先に電子メールで送信するという連携サービスを提供することを考える。指示入力装置 1 0 は、各サーバ 2 5 a、2 5 b の処理内容の記述を、それぞれ対応するサーバ 2 5 a、2 5 b の公開鍵で暗号化し、その各々の暗号化結果を含んだ指示書を作成して、サーバ 2 5 a に送信する。

【選択図】 図 7

特願 2 0 0 3 - 0 8 1 9 1 8

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 4 9 6]

1. 変更年月日

1 9 9 6 年 5 月 2 9 日

[変更理由]

住所変更

住 所

東京都港区赤坂二丁目 1 7 番 2 2 号

氏 名

富士ゼロックス株式会社